UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/715,346	11/17/2003	Richard Sutton	SYMAP031	2398

35833 7590 03/19/2008

VAN PELT & YI LLP
10050 N. FOOTHILL BLVD.
SUITE 200
CUPERTINO, CA 95014

EXAMINER	
LEMMA, SAMSON B	
ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
03/19/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/715,346	SUTTON ET AL.	
	Examiner	Art Unit	
	Samson B. Lemma	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 November 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-11 and 13-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-11 and 13-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in reply to an amendment filed on November 19, 2007. Claim 12 is canceled, thus **claims 1-11 and 13-23** are pending/examined.

2. Independent claims **1, 22 and 23 and dependent claims 5 and 13** are amended.

Priority

3. This application does not claim priority of any application. Therefore, the effective filling data for the subject matter defined in the pending claims of this application is **November 18, 2003.**

Response to Arguments

4. Applicant's argument filed on November 19, 2007 have been fully considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. **Claims 1-5, 13-23** are rejected under 35 U.S.C. 102(e) as being unpatentable over by **Campbell et al.** (hereinafter referred to as **Campbell**) (U.S. Publication No. 2004/0003284 A1) (filed on Jun 26, 2002) in view of Boulanger et al. (hereinafter referred to as Boulanger) (U.S. Publication No. 2005/0027854 A1) (filed on 07/29/2003)

7. As per independent claims 1,22 and 23 and dependent claims 13-16 Campbell discloses a method for tracking a virus [Abstract] *(As it has been disclosed on the abstract the method is used to detect possible virus attacks and identify the source of the attacks within a computer network")* **comprising:**

- **Copying from a first packet received at a destination host to which the first packet is addressed an information including a sender information usable to determine as sending source that addressed and sent the first packet to the destination host** *[Abstract and paragraph 0025-0026] (On abstract and on paragraph 0026, it has been disclosed that in an off-line scan mode, the* ***packets are copied*** *and are passing through the switch and on paragraph 0025, it has been disclosed that because the ports of a network switch are directly connected to respective physical computers in the network, the detection of a virus signature or a virus attack pattern by the switch allows an* ***unambiguous***

determination of the source of the network traffic *that contains the virus attack and this implies that the detection of the virus includes getting information about the packets including the source and the destination address of the packets and such information being part of the packets are also copied.* ***Campbell on paragraph 0017, the last 4 lines discloses the following. "*** *A switching control component 78 of the switch controls the routing of network communication packets between the ports of the switch. When a packet is received at a port, the switching control 78* ***identifies a destination port for that packet from information in the packet,*** *and forwards the packet to the destination port." Therefore it is undoubtedly clear that a destination/source address is something which can be/is read from the packet itself. Furthermore Campbell on paragraph 0027, discloses the following.*

"To scan a packet, the virus scanner 126 reads the content of the packet and matches it against the virus signatures stored in the virus information database 100 and determines whether ***this packet and previous packets from the same port together*** *show a discernable pattern of virus attacks."*

This implies the fact that virus information database contains the source address of the packets with the corresponding signature so that when the scanner reads the content of the new packets which

includes the source address of the packets and matches it against the virus signatures stored in the database and determines whether this new packet and the pervious packets from the same port/source address show a discernable pattern of virus attacks.)

- **Passing through a second packet associated with the first packet** *[Abstract and paragraph 0025-0026] (On abstract and on paragraph 0026, it has been disclosed that in an In an off-line scan mode, the* ***packets are copied*** *and are passing through the switch and on paragraph 0025, it has been disclosed that because the ports of a network switch are directly connected to respective physical computers in the network, the detection of a virus signature or a virus attack pattern by the switch allows an* ***unambiguous determination of the source of the network traffic*** *that contains the virus attack and this implies that the detection of the virus includes getting information about the packets including the source and the destination address of the packets and such information being part of the packets are also copied. It is inherently included that the second packets or the subsequent packets which has the same source and destination address will not be copied or saved but will be passed through with out being scanned since it is unnecessary to do so. Or the second packets which is interpreted by the office as those packets which are received when the system is in*

an on-line scan mode are instead scanned dynamically and forwarded to their destination ports without being copied or saved and this meets the limitation, "passing through a second packet"*);*

- **Saving the copied information;** [Abstract] *(As it disclosed on the abstract, In an off-line scan mode, a copy of the packets passing throug**h the switch is saved into a packet queue for scanning**.)*

- **Determining whether an infection has been received, wherein the infection is associated with a network transmission, with which the first and second packets are associated; [paragraph 0027]** *(In one embodiment, the virus scanner 126 of the network switch 72 processes the packets 122 in the packet queue 120 on a first-in-first-out (FIFO) basis. In other words, the oldest packet in the queue 120 will be scanned first for virus signatures or attack patterns. To scan a packet, the virus scanner 126 reads the content of the packet and matches it against the virus signatures stored in the virus information database 100 **and determines whether this pac**ket and previous packets from the same port together show a discernable pattern of virus attacks.)* **and**

• **retrieving the saved information. [paragraph 0028] (** When the network switch 72 detects a virus signature or attack pattern in the network packets passing through its ports, it can take various steps to prevent the spreading of the virus. In a preferred embodiment, depending on the current alert set by the system administrator, the network switch 72 performs one of three actions. And on the same paragraph the following has been disclosed. "The network switch can alert the computer from which the virus attack originated that it is infected, or alert the system administrator that the computer is infected," and in order to alert the computer from which the virus attack is originated the system has to retrieve the source address and other information from the packets that are already copied and saved and finally scanned]**; and**

• **Using the saved information to identify and take a responsive action with respect to the sending source.** **[**Paragraph 0027-0028]

Campbell does not explicitly disclose:

Performing virus detection at a destination host to which the first packet is addressed, and determining the source of an attack based on a sender information copied from a received first packet.

However, in the same field of endeavor, **Boulanger** discloses performing virus detection at a destination host to which the first packet is addressed, and determining the source of an attack based on a sender information copied from a received first packet. *[See paragraph 0030-0031, 0011-0012 and Fig. 11, 0035, for instance how the intrusion detection program could be installed at the victim location]*

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the feature of performing virus detection at a destination host to which the first packet is addressed, and determining the source of an attack based on a sender information copied from a received first packet as per teachings of **Boulanger** into the method taught by **Campbell**, in order to provide a secure intrusion detection system to protect from malicious attacks launched by hackers at the victim location. [See for instance **Boulanger** paragraph 0002 and claim 30]

8. **As per claim 2-4 and 17-21 the combination of Campbell and Boulanger discloses a** method as applied to claims above. Furthermore **Boulanger** discloses the method wherein, the information includes a file system location/includes a file name or

information includes a network address of a source computer. *[See paragraph 0030-0031, 0011-0012 and claim 30]*

9. **As per claim 5 the combination of Campbell and Boulanger discloses a** method as applied to claims above. Furthermore **Boulanger** discloses the method wherein, the information is saved on a destination computer [*See paragraph 0030-0031, 0011-0012 and claim 30]*

10. **Claims 6-11** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Campbell et al.** (hereinafter referred to as **Campbell**) (U.S. Publication No. 2004/0003284 A1) (filed on Jun 26, 2002) in view of Boulanger et al. (hereinafter referred to as Boulanger) (U.S. Publication No. 2005/0027854 A1) (filed on 07/29/2003) and in further view of Lahti et al (hereinafter referred to as **Lahti**) (U.S. Publication No. 2005/0033975 A1) (filed on August 8, 2002)

11. **As per dependent claims 6-11 Campbell discloses a** method for tracking a virus [Abstract] *(As it has been disclosed on the abstract*

the method is used to detect possible virus attacks and identify the source of the attacks within a computer network") **comprising:**

- **Copying from a first packet received at a destination host to which the first packet is addressed an information including a sender information usable to determine as sending source that addressed and sent the first packet to the destination host** *[Abstract and paragraph 0025-0026] (On abstract and on paragraph 0026, it has been disclosed that in an off-line scan mode, the* ***packets are copied*** *and are passing through the switch and on paragraph 0025, it has been disclosed that because the ports of a network switch are directly connected to respective physical computers in the network, the detection of a virus signature or a virus attack pattern by the switch allows an* ***unambiguous determination of the source of the network traffic*** *that contains the virus attack and this implies that the detection of the virus includes getting information about the packets including the source and the destination address of the packets and such information being part of the packets are also copied.* ***Campbell on paragraph 0017, the last 4 lines discloses the following. "*** *A switching control component 78 of the switch controls the routing of network communication packets between the ports of the switch. When a packet is received at a port, the switching control 78*

identifies a destination port for that packet from information in the packet, *and forwards the packet to the destination port." Therefore it is undoubtedly clear that a destination/source address is something which can be/is read from the packet itself. Furthermore Campbell on paragraph 0027, discloses the following.*

"To scan a packet, the virus scanner 126 reads the content of the packet and matches it against the virus signatures stored in the virus information database 100 and determines whether ***this packet and previous packets from the same port together*** *show a discernable pattern of virus attacks."*

This implies the fact that virus information database contains the source address of the packets with the corresponding signature so that when the scanner reads the content of the new packets which includes the source address of the packets and matches it against the virus signatures stored in the database and determines whether this new packet and the pervious packets from the same port/source address show a discernable pattern of virus attacks.)

- **Passing through a second packet associated with the first packet** *[Abstract and paragraph 0025-0026] (On abstract and on paragraph 0026, it has been disclosed that in an In an off-line scan mode, the* ***packets are copied*** *and are passing through the switch and on paragraph 0025, it has been disclosed that because*

the ports of a network switch are directly connected to respective physical computers in the network, the detection of a virus signature or a virus attack pattern by the switch allows an ***unambiguous determination of the source of the network traffic*** *that contains the virus attack and this implies that the detection of the virus includes getting information about the packets including the source and the destination address of the packets and such information being part of the packets are also copied. It is inherently included that the second packets or the subsequent packets which has the same source and destination address will not be copied or saved but will be passed through with out being scanned since it is unnecessary to do so. Or the second packets which is interpreted by the office as those packets which are received when the system is in an on-line scan mode are instead scanned dynamically and forwarded to their destination ports without being copied or saved and this meets the limitation,* "passing through a second packet"*);*

- **Saving the copied information;** [Abstract] *(As it disclosed on the abstract, In an off-line scan mode, a copy of the packets passing throug****h the switch is saved into a packet queue for scanning****.)*

- **Determining whether an infection has been received, wherein the infection is associated with a network transmission, with which the first and second packets are associated; [paragraph 0027]** *(In one embodiment, the virus scanner 126 of the network switch 72 processes the packets 122 in the packet queue 120 on a first-in-first-out (FIFO) basis. In other words, the oldest packet in the queue 120 will be scanned first for virus signatures or attack patterns. To scan a packet, the virus scanner 126 reads the content of the packet and matches it against the virus signatures stored in the virus information database 100* ***and determines whether this pac****ket and previous packets from the same port together show a discernable pattern of virus attacks.)*

and

- **retrieving the saved information. [paragraph 0028] (** When the network switch 72 detects a virus signature or attack pattern in the network packets passing through its ports, it can take various steps to prevent the spreading of the virus. In a preferred embodiment, depending on the current alert set by the system administrator, the network switch 72 performs one of three actions. And on the same paragraph the following has been disclosed. "The network switch can alert the computer from which the virus attack originated that it is infected, or alert the system

administrator that the computer is infected," and in order to alert the computer from which the virus attack is originated the system has to retrieve the source address and other information from the packets that are already copied and saved and finally scanned.]

- **Using the saved information to identify and take a responsive action with respect to the sending source.**

[Paragraph 0027-0028]

Campbell does not explicitly disclose

Performing virus detection at a destination host to which the first packet is addressed, and determining the source of an attack based on a sender information copied from a received first packet.

However, in the same field of endeavor, **Boulanger** discloses performing virus detection at a destination host to which the first packet is addressed, and determining the source of an attack based on a sender information copied from a received first packet. *[See paragraph 0030-0031, 0011-0012 and claim 30 "see for instance how the intrusion detection program could be installed at the victim location]*

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the feature of performing virus detection at a destination host to which the first

packet is addressed, and determining the source of an attack based on a sender information copied from a received first packet as per teachings of **Boulanger** into the method taught by **Campbell**, in order to provide a secure intrusion detection system to protect from malicious attacks launched by hackers at the victim location. [See for instance **Boulanger** paragraph 0002 and claim 30]

The combination of **Campbell** and **Boulanger** does not explicitly teach that the determination of when a virus has been received is performed when an attempt to open/read/write/create/access/delete a file occurs.

However, in the same field of endeavor, **Lahti discloses** that Various anti-virus applications are available on the market today. These tend to work by maintaining a database of signatures or fingerprints for known viruses. With a "real time" scanning application, when a user **tries to perform an operation on a file, e.g. open, save, or copy, the request is redirected to the anti-virus application.** If the application has no existing record of the file, the file is scanned for known virus signatures. If a virus is identified in a file, the anti-virus application reports this to the user, for example by displaying a message in a pop-up window. [Paragraph 0004]

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the feature of determining when a virus has been received is performed when an attempt open/read/write/create/access a file occurs as per teachings of **Lahti** into the combination of the method as taught by **Campbell and Boulanger** to provide security by preventing the propagation of the virus by adding the identity of the infected file to a register of infected files and when a subsequent operation on the file is requested, the anti-virus application first checks the register to see if the file is infected If it is infected, it can easily denies the access.[See **Lahti** paragraph 0004]

Conclusion

12. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).
A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached

on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/S. B. L./
Samson B Lemma
Examiner, Art Unit 2132
03/05/2008

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2132